UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DEBORAH HARRINGTON, individually and on behalf of all others similarly situated, Plaintiff -against- ELEKTA, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Deborah Harrington, individually and on behalf of all others similarly situated, by and through her attorneys, Finkelstein, Blankinship, Frei-Pearson & Garber, LLP; Keller Lenkner LLC; Gray, Rust, St. Amand, Moffett & Brieske, LLP; and Fish Potter Bolaños, P.C. and for her class action complaint against Defendant Elekta, Inc., respectfully alleges, upon her own knowledge or, where she lacks personal knowledge, upon information and belief including the investigation of her counsel, as follows:

INTRODUCTION

1. Plaintiff Deborah Harrington ("Plaintiff" or "Ms. Harrington") brings this class action lawsuit on behalf of herself and all others similarly situated against Defendant Elekta, Inc. ("Defendant" or "Elekta") as a result of Defendant's failure

to safeguard and protect the confidential information of Ms. Harrington and the other members of the Class – including names, dates of birth, Social Security Numbers, health insurance information, medical record numbers, and clinical information related to treatment – in Defendant's custody, control, and care that can be used to perpetrate identity theft (the "Sensitive Information").

2. Plaintiff is a former patient of Northwestern Memorial HealthCare ("NMHC"). As a condition of receiving medical treatment from NMHC, Plaintiff was required to and did supply Sensitive Information to Defendant, including, but not limited to, her Social Security Number, date of birth, financial information, health insurance information, and other personal private data.

3. NMHC, along with numerous other healthcare providers, utilized Elekta as a vendor to provide a cloud-based platform to store and transmit records electronically. Elekta stored Plaintiff's and Class Members' Sensitive Information on its electronic database.

4. Unbeknown to Plaintiff, Elekta did not have sufficient cyber-security procedures and policies in place to safeguard the Sensitive Information it possessed. As a result, cybercriminals were able to gain access to Elekta's systems between approximately April 2, 2021, and April 20, 2021 as part of a "ransomware" attack. This attack allowed the cybercriminals to gain access to and copy the Sensitive

Information of hundreds of thousands of Class Members, including Plaintiff and approximately 201,196 other patients from NMHC alone, that was stored in Elektra's database (the "Data Breach"). Plaintiff and members of the proposed Class have suffered damages as a result of the unauthorized and preventable disclosure of their Sensitive Information.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity protections and protocols that were necessary to protect the Sensitive Information of patients who entrusted it into Defendant's custody and care.

6. This lawsuit seeks to redress Defendant's unlawful disclosure of the Sensitive Information of all persons affected by the Data Breach. Elekta's unlawful disclosure of this Sensitive Information to cybercriminals has caused actual harm to Plaintiff and Class Members and placed them at an increased risk of identity theft, for which they must now undertake additional security measures to minimize.

PARTIES

7. Plaintiff Deborah Harrington is and was a resident of Oak Park, Illinois, in Cook County, who is and was a patient of one of Elekta's clients, NMHC, prior to the Data Breach, and whose Sensitive Information was compromised in the Data Breach.

8. Defendant Elekta, Inc. is a Swedish radiation therapy, radiosurgery, and related equipment data services provider that is incorporated and doing business in Dunwoody, Georgia.

JURISDICTION AND VENUE

9. This Court has jurisdiction over this matter and all causes of action asserted herein under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because at least one member of the Class is a citizen of a different state than Defendant, there are more than 100 putative Class Members, and the amount in controversy, exclusive of interest and costs, is in excess of $5 million.

10. This Court has jurisdiction over Defendant because it has conducted and continues to conduct business in the State of Georgia, it has sufficient minimum contacts in Georgia, and it maintains its United States headquarters in Dunwoody, Georgia, in DeKalb County.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Elekta's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

THE RISKS OF MEDICAL DATA BREACHES IS WELL KNOWN

12. Defendant had obligations created by contract, industry standards, common law, and representations it made to keep Plaintiff's and Class Members'

Sensitive Information confidential and to protect it from unauthorized access and disclosure.

13. Defendant was well aware that data in its care would be stolen if it did not take adequate precautions. Indeed, data breaches occur all too frequently in Defendant's industry and are well publicized.

14. Defendant's data security obligations are and were particularly important given the substantial increase in cyberattacks and/or data breaches widely reported on in the last few years. In fact, in the wake of this rise in data breaches, the Federal Trade Commission has issued an abundance of guidance for companies and institutions that maintain individuals' Sensitive Information.[1]

15. One of the primary methods of accomplishing a data hack is through malware, defined by wikipedia.org as "any software intentionally designed to cause damage to a computer, server, client, or computer network.[2] One leading financial journal estimated that upwards of one million malware threats are created *every day*.[3]

---

[1] *See, e.g., Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[2] https://en.wikipedia.org/wiki/Malware, last accessed on May 2, 2019

[3] https://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

Ransomware, which prevents authorized users from accessing infected files or systems to extort payment, is one type of malware.

16. Medical providers have been a primary target of hackers because of the rich cache of Sensitive Information which patients must disclose to their various medical providers.

17. A comprehensive study undertaken by the JAMA Network found that data breaches exposing medical records increased from 199 hacks in 2010 to 344 hacks in 2017, with the corresponding number of compromised medical records increasing from 5.9 million to 176.3 million, respectively.[4]

18. Another authoritative study in 2016 found that data breaches at healthcare organizations were on the increase, that the organizations thought they were more vulnerable to data breach than other organizations, but that these organizations were unprepared to address new threats.[5] The study also found that

[4] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6233611/, last accessed May 2, 2019

[5] https://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1?q=library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1, cited in New York State Bar Association Journal, May 2019, p.15

healthcare organizations' biggest concern in cybersecurity was employee negligence, and that the majority of data breaches were caused by criminal acts.[6]

19. Indeed, according to a report by Risk Based Security, Inc., by the end of June 2020 was already the "worst year on record" in terms of records exposed in data breaches.[7]

20. Therefore, Defendant clearly knew or should have known of the risks of data breaches and thus should have ensure that adequate protections were in place.

DATA BREACHES LEAD TO IDENTITY THEFT

21. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victims' name, lock the victim out of his or her financial or social media

[6] https://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1?q=library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1, p. 3, 5

[7] *See 2020 Q3 Report*, Risk Based Security, *available at* https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf.

accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[8]

22. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[9] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

23. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[10]

24. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact to their credit. Identity thieves

---

[8] *See* https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/ (last accessed May 7, 2019).

[9] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* <https://www.gao.gov/new.items/d07737.pdf> (last visited June 3, 2019).

[10] *Id.* at 2, 9.

use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

25. There may be a time lag between when sensitive information is stolen and when it is used. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

26. With access to an individual's Sensitive Information, cyber criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security Number to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the

[11] *Id*. at 29 (emphasis added).

victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[12]

27. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security Numbers, and other Sensitive Information directly on various Internet websites, making the information publicly available.

DEFENDANT ALLOWED CRIMINALS TO OBTAIN PLAINTIFF AND THE CLASS MEMBERS' SENSITIVE INFORMATION.

28. Due to inadequate security against unauthorized intrusions, hackers breached Defendant's computer systems on or about April 2, 2021, resulting in the criminals unlawfully obtaining patients' Sensitive Information, including Social Security Numbers, dates of birth, medical treatment information, medical record numbers, and health insurance information or policy numbers. As part of this Data Breach, the hackers removed and/or encrypted Defendant's files, in what is commonly referred to as a "ransomware" attack.

[12] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 28, 2019).

DEFENDANT'S REPRESENTATIONS AND NEGLIGENT FAILURE TO MEET THEM

29. As part of the regular course of its business, Defendant maintains immense volumes of patients' Sensitive Information, provided by its clients. As such, Defendant is well aware of the value of healthcare patients' data and that such Sensitive Information is highly sought by cybercriminals.

30. Defendant represents that it is able to "protect your data" through, among other services and measures:

- Improved data securing using Azure advanced security and [artificial intelligence] along with multi-layer threat protection;
- Better data organization leveraging modular infrastructure as code;
- Better data organization leveraging modular infrastructure as code;
- Disk encryption at rest.

https://www.elekta.com/software-solutions/cloud-solutions/ (last accessed Sept. 23, 2021). Defendant further represents that "safeguarding your clinical data is our highest priority." *Id*.

31. Yet, despite these public representations which lead clients and customers to reasonably believe that patients' Sensitive Information would be safe in Defendant's custody and care, on or around April 2, 2021, Defendant allowed cybercriminals to breach and access Defendant's systems and database, including the Sensitive Information contained therein, in a ransomware attack.

32. Defendant's security failure in permitting the Data Breach demonstrates that it failed to honor its duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting Plaintiff's and the Class Members' Sensitive Information;

c. Properly monitoring its own data security systems for existing intrusions; and

d. Ensuring that agents, employees, and others with access to Sensitive Information employed reasonable security procedures.

33. Plaintiff and all members of the Class have consequently suffered harm by virtue of the compromise and exposure of their Sensitive Information – including, but not limited to, (i) an imminent risk of future identity theft; (ii) lost time and money expended to mitigate the threat of identity theft; (iii) diminished value of personal information; and (iv) a loss of privacy. Plaintiff and all members of the proposed Class are and will continue to be at imminent risk for tax fraud and identify theft and the attendant dangers thereof for the rest of their lives because their

Sensitive Information, including Social Security Numbers and healthcare information, is in the hands of cybercriminals.

CLASS ALLEGATIONS

34. This action is brought on behalf of Plaintiff, and all similarly situated persons pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3). The Class is defined as:

> All persons whose Sensitive Information stored on Defendant's databases or systems was exposed to unauthorized access by way of the data breach of Defendant's computer system on or about April 2, 2021.

35. Plaintiff reserves the right to amend the above definition, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

36. Plaintiff is a member of the Class.

37. Excluded from the Class are: (i) Defendant; any entity in which Defendant has a controlling interest; the officers, directors, and employees of Defendant; and the legal representatives, heirs, successors, and assigns of Defendant; (ii) any judge assigned to hear this case (or any spouse or family member of any assigned judge); (iii) any juror selected to hear this case; and (iv) any and all legal representatives (and their employees) of the parties.

38. This action seeks both injunctive relief and damages.

39. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

40. **Numerosity of the Class.** According to contemporaneous reporting on the Data Breach, the Data Breach affected at least tens of thousands of individuals. Therefore, the members of the Class are so numerous that their individual joinder is impracticable. The precise number of persons in the Class and their identities and addresses may be ascertained or corroborated from Defendant's records. If deemed necessary by the Court, members of the Class may be notified of the pendency of this action.

41. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendant's data security systems prior to the Data Breach met the requirements of relevant laws;

b. Whether Defendant's data security systems prior to the Data Breach met industry standards;

c. Whether Plaintiff's and other Class Members' Sensitive Information was compromised in the Data Breach; and

d. Whether Plaintiff and other Class Members are entitled to damages as a result of Defendant's conduct.

42. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same

legal theories and same violations of law. Plaintiff's grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendant.

43. **Adequacy.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. Her interests do not conflict with the interests of the Class.

44. Plaintiff and her chosen attorneys – Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG"); Keller Lenkner, LLC ("Keller Lenkner"); Gray, Rust, St. Amand, Moffett & Brieske, LLP; and Fish Potter Bolaños, P.C. – are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint.

45. FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. FBFG's attorneys are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class Members. Finally, FBFG possesses the financial resources necessary to ensure that the litigation will not be hampered by a lack of financial capacity and is willing to absorb the costs of the litigation.

46. Keller Lenkner is the 2021 Trial Strategy Innovation Law Firm of the Year, as named by The National Law Journal and American Lawyer Media. Keller Lenkner is a national firm that has secured recovery on behalf of hundreds of thousands of plaintiffs across America and is dedicated to zealously representing members of the Class. Keller Lenkner has the financial resources and staffing necessary to support the costs of this litigation.

47. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large a number of injured persons, to keep the courts from becoming paralyzed by hundreds – if not thousands – of repetitive cases, and to reduce transaction costs so that the injured Class Members can obtain the most compensation possible.

48. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will

promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only patients whose Sensitive Information was exposed in the Data Breach, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

49. In addition, Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or equitable relief with respect to the Class.

FIRST CAUSE OF ACTION

NEGLIGENCE IN THE HANDLING OF PLAINTIFF'S AND THE CLASS'S SENSITIVE INFORMATION

50. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

51. Defendant owed a duty to Plaintiff and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiff's and Class Members' Sensitive Information within its control from being compromised by or being accessed by unauthorized third parties. This duty included, among other things, maintaining adequate control over its computer systems and network so as to prevent unauthorized access thereof.

52. Defendant owed a duty of care to the Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that its computer systems adequately protected the Sensitive Information of the individuals who entrusted it to the Defendant.

53. Defendant's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between it and its patients, which is recognized by laws including, but not limited to, HIPAA. Only Defendant was in a position to ensure that its systems were sufficient to protect against harm to Plaintiff and the members of the Class from the Data Breach.

54. Defendant's duty to use reasonable security measures also arose under HIPAA, pursuant to which Defendant is required to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The Sensitive Information at issue in this case includes "protected health information" within the meaning of HIPAA.

55. In addition, Defendant had a duty to use reasonable security measures under Section A of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

56. Defendant's duty to use reasonable care in protecting the Sensitive Information arose not only as a result of the common law and the statutes and regulations described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of confidential information.

57. Defendant breached its common law, statutory, and other duties – and thus, was negligent – by failing to use reasonable measures to protect the patients'

Sensitive Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and the Class Members' Sensitive Information;

b. failing to adequately monitor the security of its networks and systems;

c. allowing unauthorized access to Plaintiff's and the Class Members' Sensitive Information; and

d. failing to warn Plaintiff and other Class Members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

58. Defendant owed a duty of care to the Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

59. It was foreseeable that Defendant's failure to use reasonable measures to protect Sensitive Information and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

60. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly

impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

61. Defendant knew or reasonably should have known of the inherent risks in collecting and storing the Sensitive Information of Plaintiff and members of the Class and the critical importance of providing adequate security of that information, yet despite the foregoing had inadequate cyber-security systems and protocols in place to secure the Sensitive Information.

62. As a result of the foregoing, the Defendant unlawfully breached its duty to use reasonable care to protect and secure the Sensitive Information of Plaintiff and the Class.

63. Plaintiff and members of the Class reasonably relied on the Defendant to safeguard their information, and while Defendant was in a position to protect against harm from a data breach, Defendant negligently and carelessly squandered

that opportunity. As a proximate result, Plaintiff and members of the Class suffered and continue to suffer the consequences of the Data Breach.

64. Defendant's negligence was the proximate cause of harm to Plaintiff and members of the Class.

65. Had Defendant not failed to implement and maintain adequate security measures to protect the Sensitive Information of medical patients, the Plaintiff's and Class Members' Sensitive Information would not have been exposed to unauthorized access and stolen, and they would not have suffered any harm.

66. However, as a direct and proximate result of Defendant's negligence, Plaintiff and members of the Class have been seriously and permanently damaged by the Data Breach. Specifically, Plaintiff and members of the Class have been injured by, among other things; (1) the loss of the opportunity to control how their Sensitive Information is used; (2) diminution of value and the use of their Sensitive Information; (3) compromise, publication and/or theft of the Plaintiff's and the Class Members' Sensitive Information; (4) out-of-pocket costs associated with the prevention, detection and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with their efforts expended and the loss of productivity from addressing as well as attempting to mitigate the actual and future consequences of the breach including, but not

limited to, efforts spent researching how to prevent, detect, and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased cost of the use, the use of credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised Sensitive Information to open new financial and/or healthcare and/or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, healthcare or medical accounts and associated lack of access to funds while proper information is confirmed and corrected and/or imminent risk of the foregoing; (9) continued risks to their Sensitive Information, which remains in the Defendant's possession and may be subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its possession; and (10) future costs in terms of time, effort and money that will be spent trying to prevent, detect, contest and repair the effects of the Sensitive Information compromised as a result of the Data Breach as a remainder of the Plaintiff's and Class Members' lives.

67. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

SECOND CAUSE OF ACTION

INTRUSION UPON SECLUSION / INVASION OF PRIVACY

68. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

69. The Restatement (Second) of Torts states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977)

70. Plaintiff and Class Members had a reasonable expectation of privacy in the Sensitive Information that Defendant mishandled. Plaintiff and Class Members maintain a privacy interest in their Sensitive Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

71. Plaintiff's and Class Members' Sensitive Information was contained, stored, and managed electronically in Defendant's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities, including Social Security numbers and medical treatment information.

72. Additionally, Plaintiff's and Class Members' Sensitive Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Sensitive Information for fraud, identity theft, and other crimes without their knowledge and consent.

73. Defendant unlawfully intruded upon Plaintiff's and Class Members' solitude, seclusion, or private affairs. Defendant's disclosure of Plaintiff's and Class Members' Sensitive Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Personal Information is offensive to a reasonable person.

74. Defendant's disclosure of Plaintiff's and Class Members' Sensitive Information to unauthorized third parties permitted the physical and electronic intrusion into Plaintiff's and Class Members' private quarters where their Sensitive Information was stored and disclosed private facts about them (including their Social Security numbers) into the public domain (in this case, the dark web).

75. In failing to protect Plaintiff's and Class Members' Sensitive Information, and in intentionally misusing and/or disclosing their Sensitive Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

76. Plaintiff and Class Members have been damaged by Defendant's conduct, by incurring the harms and injuries arising from the Data Breach now and in the future. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

THIRD CAUSE OF ACTION

DECLARATORY JUDGMENT

77. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

78. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201. As previously alleged and pleaded, Defendant owes duties of care to Plaintiff and Class Members that require it to adequately secure their Sensitive Information.

79. Defendant still possesses the Sensitive Information of Plaintiff and Class Members.

80. Plaintiff therefore seeks a declaration that (1) Defendant's existing security measures do not comply with its obligations to Plaintiff and Class Members; and (2) to comply with its duties of care, Elekta must implement and maintain reasonable security measures, including, but not limited to:

- Ordering Defendant to engage third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;
- Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;
- Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
- Ordering that Defendant purge, delete, and destroy in a reasonably secure manner any Sensitive Information not necessary for its provisions of services;
- Ordering that Defendant conduct regular database scanning and securing checks;
- Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to

identify and contain a breach when it occurs and what to do in response to a breach;

- Ordering Defendant to implement and enforce adequate retention policies for Sensitive Information, including destroying Sensitive Information as soon as it is no longer necessary for it to be retained; and
- Ordering Defendant to meaningfully educate those utilizing its services, including Employers and their employees, about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

81. Plaintiff and the Class have no other adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Deborah Harrington demands judgment on behalf of herself and the Class as follows:

a. Certifying that the action may be maintained as a class action and appointing the named Plaintiff to be class representative and the undersigned counsel to be Class Counsel;

b. Requiring that Defendant pay for notifying the members of the Class of the pendency of this suit;

c. Awarding Plaintiff and the Class appropriate relief, including actual damages, compensatory damages, and punitive damages on the First and, Second Causes of Action;

d. Awarding injunctive relief on the Third Cause of Action requiring Defendant to safeguard the Sensitive Information in its custody and care;

e. Awarding Plaintiff and the Class prejudgment and post-judgment interest;

f. Awarding Plaintiff and the Class their attorneys' fees and costs pursuant to applicable laws, together with their costs and disbursements of this action; and

g. Awarding such other and further relief as the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of the Class, demands a trial by jury as to all issues triable of right.

Dated: September 28, 2021

Respectfully Submitted,

By: */s/ David C. Sawyer*
David C. Sawyer
Georgia Bar No. 751032

GRAY, RUST, ST. AMAND, MOFFETT & BRIESKE, LLP
1700 Salesforce Tower Atlanta
950 East Paces Ferry Road
Atlanta, Georgia 30326
Tel: (404) 870-7439
dsawyer@grsmb.com

Todd S. Garber (*pro hac vice* forthcoming)
Andrew C. White (*pro hac vice* forthcoming)
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com
awhite@fbfglaw.com

Seth A. Meyer (*pro hac vice* forthcoming)
Alex J. Dravillas (*pro hac vice* forthcoming)
KELLER LENKNER LLC
150 N. Riverside, Suite 4270
Chicago, Illinois 60606
Tel: (312) 741-5220
sam@kellerlenkner.com
ajd@kellerlenkner.com

Mara Baltabols (*pro hac vice* forthcoming)
FISH POTTER BOLAÑOS, P.C.
200 E. 5th Ave, Suite 123
Naperville, IL 60563
Tel: (630) 364-4061
mbaltabols@fishlawfirm.com

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DEBORAH HARRINGTON, individually and on behalf of all others similarly situated, Plaintiff -against- ELEKTA, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

LR 7.1(D) CERTIFICATE OF FONT COMPLIANCE

I hereby certify that the foregoing has been prepared with one of the font and point selections approved by the Court in Local Rule 5.1(C), Northern District of Georgia, specifically Times New Roman 14 point.

Dated: September 28, 2021

Respectfully Submitted,

By: */s/ David C. Sawyer*
David C. Sawyer
Georgia Bar No. 751032
GRAY, RUST, ST. AMAND, MOFFETT & BRIESKE, LLP
1700 Salesforce Tower Atlanta
950 East Paces Ferry Road
Atlanta, Georgia 30326
Tel: (404) 870-7439
dsawyer@grsmb.com